Claims

1. In a cryptographic system having one of a plurality of states, an interactive method of controlling the transition of said system from an existing state to a future state under control of one or more authorities, said method being performed by said cryptographic system and comprising the steps of:

storing control information specifying permissible future states based on a current state and a requesting authority;

receiving a query from an authority as to the current state of the cryptographic system;

providing a reply to said authority in response to said query, said reply containing state information regarding the current state of said cryptographic system and reply authentication information for enabling said authority to determine whether said reply originated from said cryptographic system;

receiving a request from an authority to change the current state of the cryptographic system, said request containing state change information indicating a proposed future state of said cryptographic system and request authentication information for enabling said cryptographic system to determine whether said request originated from said authority;

determining using said request authentication information whether said request originated from said authority; and

performing said request only if the request is determined to have originated from said authority and the proposed future state is a permissible future state as specified by said control information.

2. The method of claim 1 in which said reply authentication information comprises a digital signature.

3. The method of claim 2, further comprising the step of:

storing a private key in the cryptographic system, said private key being used for generating said digital signature.

4. The method of claim 1 in which said query includes a unique query value, said reply authentication information being generated on said reply including said query value.

5. The method of claim 1, further comprising the step of:

storing a unique transaction value in the cryptographic system, a request from an authority including a transaction value, a request being performed only if the transaction value in the request is the same as the transaction value in the cryptographic system, said transaction value in the cryptographic system being updated to a new unique value upon performance of a request.

6. The method of claim 5 in which said transaction value comprises a random part and a sequential part, said sequential part being incremented upon performance of a request.

7. The method of claim 1 in which said request authentication information comprises a digital signature.

8. The method of claim 7, further comprising the step of:

storing a public key for an authority, said request being authenticated by means of said public key.

9. The method of claim 1 in which all or a portion of a proposed future state is stored in a pending command register.

10. The method of claim 1 in which said cryptographic processor transitions from said existing state to said future state through one or more intermediate states, said intermediate states being represented at least in part as a series of single bits in a signature summary mask, each bit representing the concurrence of an authority to continue the process of intermediate states toward said future state.

11. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform the method steps of claim 1.

12. In a cryptographic system having one of a plurality of states, apparatus for interactively controlling the transition of said system from an existing state to a future state under control of one or more authorities, said apparatus being associated with said cryptographic system and comprising:

means for storing control information specifying permissible future states based on a current state and a requesting authority;

means for receiving a query from an authority as to the current state of the cryptographic system;

means for providing a reply to said authority in response to said query, said reply containing state information regarding the current state of said cryptographic system and reply authentication information for enabling said authority to determine whether said reply originated from said cryptographic system;

means for receiving a request from an authority to change the current state of the cryptographic system, said request containing state change information indicating a proposed future state of said cryptographic system and request authentication information for enabling said cryptographic system to determine whether said request originated from said authority;

means for determining using said request authentication information whether said request originated from said authority; and

means for performing said request only if the request is determined to have originated from said authority and the proposed future state is a permissible future state as specified by said control information.

13. The apparatus of claim 12 in which said reply authentication information comprises a digital signature.

14. The apparatus of claim 12 in which said query includes a unique query value, said reply authentication information being generated on said reply including said query value.

15. The apparatus of claim 12, further comprising:

means for storing a unique transaction value in the cryptographic system, a request from an authority including a transaction value, a request being performed only if the transaction value in the request is the same as the transaction value in the cryptographic system, said transaction value in the cryptographic system being updated to a new unique value upon performance of a request.

16. The apparatus of claim 15 in which said transaction value comprises a random part and a sequential part, said sequential part being incremented upon performance of a request.

17. The apparatus of claim 12 in which said request authentication information comprises a digital signature.

18. The apparatus of claim 12 in which all or a portion of a proposed future state is stored in a pending command register.

19. The apparatus of claim 12 in which said cryptographic processor transitions from said existing state to said future state through one or more intermediate states, said intermediate states being represented at least in part as a series of single bits in a signature summary mask, each bit representing the concurrence of an authority to continue the process of intermediate states toward said future state.